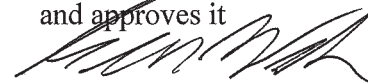


IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
HARRISONBURG DIVISION

The undersigned Assistant U.S.
Attorney has
reviewed the entire search
warrant package
and approves it



IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
GOOGLE ACCOUNT
JOEMADARATS588@GMAIL.COM, THAT
ARE STORED AT PREMISES
CONTROLLED BY GOOGLE LLC AND
GOOGLE PAYMENT CORPORATION

Case No. 5:24-mj-00063

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Steven W. Duke, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with Google Accounts connected to joemadarats588@gmail.com, ("TARGET ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Google LLC and Google Payment Corporation ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since January 2009. As such, I am a law enforcement officer of the United States within the

meaning of 18 U.S.C. § 2510(7) and am empowered by law to conduct investigations and to make arrests for offenses enumerated in 18 U.S.C. § 2516. I am currently assigned to the Winchester Resident Agency of the FBI Richmond Field Office.

3. As a Special Agent of the FBI, I have investigated violations of federal law and have gained experience and knowledge through investigations and training, and from discussions with law enforcement officers with experiences and training in investigating violations of federal law. I have been involved in the use of the following investigative techniques: interviewing victims, witnesses, and subjects; conducting physical surveillance; consensual monitoring; analyzing records associated with social media accounts, IP addresses, phone numbers, financial records, email accounts, and telephone tolls; and assisting with Title III and consensual wiretap investigations. Through my work, I have also talked to other investigators with experience investigating these types of offenses and learned about the types of evidence typically gathered from the execution of search warrants, including searches of email accounts. As a law enforcement officer, I am authorized to execute warrants issued under authority of the United States.

4. The facts in this affidavit come from a variety of sources, including: my personal observations and participation in this investigation; my training and experience; information obtained from other agents, task force officers, and witnesses; information obtained through records and databases; and other sources, which I believe to be reliable. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. This affidavit also reflects my current understanding of facts relating to this investigation, but my understanding may change in the future as the investigation proceeds. Similarly, where information contained in reports and other documents or records are referenced herein, such information is also described in sum and

substance and in relevant part only. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I have drawn from my training, experience, and knowledge of the investigation.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 115 (Threatening Federal Officials), Title 18, United States Code, Section 871 (Threatening the President of the United States and Successors to the Presidency), Title 18, United States Code, Section 875(c) (Threatening Interstate Communications), and Title 18, United States Code, Section 879 (Threatening Former Presidents and Certain Other Persons) have been committed. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

A. GETTR THREATS

8. On July 27, 2024, at 2:47 p.m. EST, Maricopa County, Arizona, Recorder’s office notified FBI Phoenix of potential threats to the Maricopa County Recorder, “Victim-1” made by

GETTR¹ username “joemadarats1”. Specifically, the “joemadarats1” GETTR account posted “someone need to remove this asshole permanently someone needs to kill this fuck.” FBI Phoenix conducted further open-source research on the “joemadarats1” GETTR account and identified further threatening statements directed at several public officials.

9. FBI Phoenix submitted legal process to GETTR and received responsive records on July 29, 2024. The responsive records from GETTR revealed approximately 4,359 posts/replies made by “joemadarats1” targeting various public officials including but not limited to: President Joseph Biden, Vice President Kamala Harris, FBI Director Christopher Wray, Victim-1, and many other public officials.

10. Specifically, President Biden was referenced 197 times by the “joemadarats1” account and included violent comments, some examples of which are below:

11/27/2023 – “JOE BIDEN AND THIS ADMIN MUST DIE”

03/11/2024 – “WE NEED TO ASSASSINATE SCUM LIKE JOE BIDEN AN HIS ADMIN”

03/11/2024 – “JOE BIDEN MUST DIE WITH HIS ADMIN”

05/18/2024 – “SUPPLY ME THE MONEY AND JOE BIDEN IS HISTORY”

05/19/2024 – “BIDEN WILL ALWAYS BE A DUMBASS WHO DOES NOT CARE FOR THIS COUNTRY HE MUST BE ASSASSINATED”

07/15/2024 – “It's the dance Joe Biden bum f***** Biden scumbag Biden f***** mumbling stuttering Biden you're a waste of life and soon your life will be wasted”

11. Vice President Kamala Harris was mentioned 19 times by the “joemadarats1” account. Some examples of the violent comments aimed at Vice President Harris are below:

¹ GETTR is a social media platform and micro blogging website. User interface and features have been described as very similar to “X”, formerly known as Twitter.

07/27/2024 – “Listen to me crappler Harris also known as cunt Harris you don't have a snowballs chance in hell which is exactly where you're going and soon I will cut your eyes out of your FUCKING head while you're alive bitch and I will make sure you suffer a slow agonizing death you piece of shit”

07/27/2024 – “Kamala Harris needs to be put on fire alive I will do it personally if no one else does it I want her to suffer a slow agonizing death”

07/27/2024 – “Harris is going to regret ever trying to become president because if that ever happened I will personally pluck out her eyes with a pair of pliers but first I will shoot and kill everyone that gets in my way that is a f***** promise”

07/27/2024 – “Just for being a Democrat you're going to die crap La Harris that's a f***** promise I'm going to find you and your f***** family and I'm going to kill you all you f***** waste of life I can't wait to rip your eyes out of your f***** head with a pair of eyes you piece of s*** and nothing but scum of the Earth and you're going to die like it”

07/27/2024 – “Crapler Harris is laying thieving piece of garbage like the rest of this administration they all need to die and they will soon”

12. The “joemadarats1” GETTR account mentioned FBI Director Christopher Wray 8 times. Some of the violent comments directed at FBI Director Wray are below:

04/12/2024 – “WRAY SHOULD DIE LIKE HE LIVES WITH HIS FINGERS UP HIS ASS”

07/27/2024 – “No Wray should be hung by his neck until he dangles to death”

07/27/2024 – “Wray is a liar and a scumbag he's also bought and sold he must pay for his actions with his life and his family's life they almost died severely”

13. Former President Barack Obama was mentioned 48 times by the “joemadarats1” GETTR account. Some examples of the violent comments directed toward former President Obama are below:

11/24/2023 – “THAT'S OBAMA FAULT AND HE SHOULD PAY WITH HIS LIFE SOON”

12/03/2023 – “NOW MAKE ALL OF THE OBAMAS PAY WITH THEIR LIVES WITH ALL THE OTHER SCUM WHO STARTED THIS”

07/27/2024 – “Soon Barack Obama and his whole family will be dead the people will kill them we will torture them to death and then we will hang them just like they belong hung in the nearest tree so everyone can see the scum that they are a naked walk over to them and carve their initials in them that is their whole family I don't give a f*** who it is but the whole family is going to die we will hunt you down and we will torture to you to death”

07/27/2024 – “I think he's taking a big chance with the CIA they work for f***** scumbag Obama he's going to die no matter what whether you getting office or not he will die and he will suffer dying Obama and his f*** disgusting vile wife boyfriend whatever the f*** you want to call him they will die the whole family will die that is my promise we the people have spoken”

07/27/2024 – “Soon Barack Obama and his whole family will be dead the people will kill them we will torture them to death and then we will hang them just like they belong hung in the nearest tree so everyone can see the scum that they are a naked walk over to them and carve their initials in them that is their whole family I don't give a f*** who it is but the whole family is going to die we will hunt you down and we will torture to you to death”

14. Other public officials referenced in threatening statements include Senators Chuck Schumer and Mitch McConnell, former Secretary of State Hillary Clinton, former President Bill Clinton, and Congresswoman Nancy Pelosi, and others.

15. On February 22, 2024, GETTR account “joemadarats1” posted on GETTR “I HAVE MY AR-15 LOCKED AND LOADED”.

B. IDENTIFICATION OF FRANK CARILLO

16. Through legal process, FBI Phoenix obtained the subscriber information from GETTR USA, Inc., for GETTR account “joemadarats1”. Based on the responsive information from GETTR with the date range of June 15, 2023, through July 28, 2024, the “joemadarats1” account was created on June 15, 2023, and is associated with the TARGET ACCOUNT (“joemadarats588@gmail.com”).

i. GETTR Location Information

17. On or about July 27, 2024, GETTR user joemadarats1 posted 46 comments to the GETTR service using two different Internet Protocol (IP) addresses. Posts submitted to GETTR by joemadarats1 between 7:36 AM - 8:07 AM used IP address 172.58.253.113, and between 9:17 AM - 7:35 PM used IP address 204.111.228.117.

18. Reviews of open-source records indicate that the service provider for IP address 172.58.253.113 is T-Mobile USA, Inc, and the service provider for 204.111.228.117 is GLO Fiber, which is a subsidiary of Shentel. GLO Fiber/Shentel was unable to provide subscriber information associated with the IP address without a port number, which GETTR did not provide to law enforcement. GETTR has advised law enforcement that it does not capture port numbers.

ii. Google Location Information

19. FBI Phoenix submitted legal process to Google, LLC, for subscriber and device information connected to the TARGET ACCOUNT. Analysis of subscriber information associated with the TARGET ACCOUNT revealed that the Google account was created on or about January 18, 2020. The name associated with the TARGET ACCOUNT is “Joe Madarats” and included a recovery email of bobungots61@gmail.com and recovery phone number of 1-610-762-5261. IP addresses associated with login activity for the TARGET ACCOUNT revealed that the account used IP address 204.111.228.117 18 times on or about July 26, 2024 - July 29, 2024. In addition, on July 29, 2024, the TARGET ACCOUNT used IP address 2607:fb91:dc4:aa75:2458:deff:fe94:c84f 1 time. Open-source records indicate that the service provider for IP address 2607:fb91:dc4:aa75:2458:deff:fe94:c84f is T-Mobile USA, Inc.

20. Google, LLC, also provided the device IMEI number 356125201089732, which belongs to an Android phone and is associated with the TARGET ACCOUNT. The device account

identifiers also provide additional email accounts connecting to the device which includes email address fcarillo@hotmail.com, among others.

21. In addition, Google, LLC, provided logins to the account associated with the TARGET ACCOUNT, which showed logins to the subject account on July 26-29, 2024, were made with IP address 204.111.228.117. This IP address is the same IP address that is seen with the threatening GETTR posts that were posted on GETTR by “joemadarats1” on July 27, 2024.

22. Analysis of the Google Location History records associated with the TARGET ACCOUNT revealed 220 records with approximate device locations for the moto g G5 device for July 27, 2024, between 4:09 AM - 10:03 PM. During this time period, all 220 records indicated that the moto g G5 device was in the immediate vicinity of the Preston Place Apartment and Townhomes located north of Airport Road near Winchester, Virginia. This area includes the residence of FRANK CARILLO, which is located at “Address-1”² in Winchester, Virginia. The entirety of the 220 records includes a display radius of 6 meters to 123 meters. Analysis of records with a display radius of 20 meters or less indicated that there are 71 records with approximate locations in the immediate vicinity of the townhomes on the west side of the same block as Address-1 (odd house numbers), which also includes the residence of CARILLO.

iii. Android Device Information

23. Analysis of Google Android Device Configuration Service Data records indicated that the mobile device used to login to the TARGET ACCOUNT was a Motorola moto g 5G uniquely identified with international mobile equipment identity (IMEI) 356125201089732. The moto g 5G was first used with Google's services on or about July 13, 2024 and continued through

² Address-1 is known to law enforcement but redacted here for privacy.

July 29, 2024. Google indicated that the subscriber identity module (SIM) card associated with the phone were encoded with a mobile country code (MCC) of 310 and mobile network code (MNC) of 240 and 260. A MCC of 310 indicates that the service provider associated with the SIM is in the United States, and both MNCs of 240 and 260 indicate that the mobile network operator is T-Mobile USA, Inc. The last data connection indicated on the Google records indicate that, at the time the Google records were obtained, the mobile device connected from IP address 2607:fb91:dc4:aa75:2458:deff:fe94:c84f. This IP address is the same IP address used to login to the TARGET ACCOUNT on July 29, 2024 and service is provided by T-Mobile USA, Inc.

24. The Google Android Device Configuration Service Data also identified 6 additional email accounts that were associated with the moto g 5G mobile device. Two of the associated email addresses include bobungots61@gmail.com (recovery email for the TARGET ACCOUNT) and fcarillo@hotmail.com.

C. SEARCH WARRANT AND USE OF TARGET ACCOUNT

25. A federal search warrant was executed at Address-1, Winchester, Virginia, on August 2, 2024. At the time the warrant was executed, CARILLO and another individual (“Witness-1”) were the only two individuals present at the residence.

i. CARILLO's Statements

26. During his initial contact with law enforcement, CARILLO asked why this was happening, and Special Agent Nicholas Olson, FBI, indicated it was related to something posted online. A short time later, CARILLO, seemingly talking to himself, stated, “...for a comment. This is ridiculous, for a comment. I guess I’m gonna need a lawyer.”

27. Additionally, CARILLO stated to another law enforcement officer, FBI Task Force Officer Zachary Hawkins, if it was “about the online stuff. I posted it.” When CARILLO overhead

law enforcement personnel discussing firearms in the residence, he indicated he had a 9mm handgun and an AR-15, which he had purchased in February.

28. Among other items, federal agents seized an RF-15 rifle³ and a 9 mm handgun from inside the residence. According to Witness-1, those particular firearms belonged to CARILLO. Witness-1 believed CARILLO purchased the handgun in 2023 and the rifle in 2024. Law enforcement also recovered more than 2,000 rounds of ammunition for the firearms, which included more than 1,000 rounds of ammunition for the AR-15.

29. Following his request for an attorney, CARILLO stated, “This is all over a comment, huh?”

30. Following his arrest, CARILLO asked, “Is [Witness-1] being arrested?” When Special Agent Steven W. Duke, FBI, replied, “I don’t know,” CARILLO stated, “[Witness-1] didn’t do anything. I made the comments.”

ii. Witness-1’s Statements

31. Witness-1 was interviewed by law enforcement. According to Witness-1, Witness-1 and CARILLO have resided in the townhouse for almost a year. During that time, no one else has lived in the residence.

32. Witness-1 advised law enforcement personnel at the scene that CARILLO utilized cellular telephone number 610-762-5261, which was the same number listed as the recovery phone number for the TARGET ACCOUNT.

³ This is a specific brand of an AR-15 rifle.

33. Witness-1 identified aliases of CARILLO as “Joe Madrats” and “Bob Ugots.” Witness-1 learned about these aliases from CARILLO. Witness-1 believed “Joe Madrats” was associated with an email address.

34. Witness-1 consented to a search of Witness-1’s cell phone. Three photos taken in May 2024 were discovered on Witness-1’s cell phone. The photos depicted the screen of another cell phone displaying email addresses and passwords. Witness-1 indicated the photos depicted CARILLO’s cell phone displaying CARILLO’s email addresses and passwords. The photos were taken to capture his passwords prior to getting a new cell phone. The photos displayed the following email addresses: the TARGET ACCOUNT, bsdmdmatter@gmail.com, cc0903571@gmail.com, bobungots61@gmail.com, and fcarillo@hotmail.com. The email addresses for the TARGET ACCOUNT and bobungots61@gmail.com sounded familiar to Witness-1.

iii. Additional Google Information

35. A preservation was served on Google for the TARGET ACCOUNT on August 1, 2024.

36. Because the TARGET ACCOUNT was the registered email account for the GETTR account “joemadarats1” that was used to threaten violence against public officials, it is reasonable to assume that the TARGET ACCOUNT contains information related to other applications that were used to make threats, as well as statements, plans, and other evidence concerning taking action on said threats.

BACKGROUND CONCERNING GOOGLE⁴

37. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

38. In addition, Google offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

39. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

40. Google advertises its services as “One Account. All of Google working for you.” Once logged into a Google Account, a user can connect to Google’s full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records

⁴ The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the “Google legal policy and products” page available to registered law enforcement at lens.google.com; product pages on support.google.com; or product pages on about.google.com.

indicating ownership and usage of the Google Account across services, described further after the description of services below.

41. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses (“recovery,” “secondary,” “forwarding,” or “alternate” email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

42. Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

43. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other

Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

44. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

45. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called

“Shared with me.” Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

46. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

47. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

48. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

49. A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both

online and brick-and-mortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.

50. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

51. Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

52. Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

53. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If

someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

54. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

55. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

56. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a

communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

57. Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

58. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found

in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

59. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

60. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

61. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (*e.g.*, information indicating a plan

to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

62. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

63. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

64. Based on the forgoing, I believe that there is probable cause to believe that evidence to show that CARILLO has violated Title 18, United States Code, Section 115 (Threatening Federal Officials), Title 18, United States Code, Section 871 (Threatening the President of the United States and Successors to the Presidency), Title 18, United States Code, Section 875(c) (Threatening Interstate Communications), and Title 18, United States Code, Section 879 (Threatening Former Presidents and Certain Other Persons) will be found in the TARGET ACCOUNT. I request that the Court issue the proposed search warrant.

65. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then

compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

66. Based on the forgoing, I request that the Court issue the proposed arrest warrant.

OATH

I declare under penalty of perjury that the foregoing is true and correct.

Respectfully submitted,

s/Steven W. Duke
Steven W. Duke, Special Agent
Federal Bureau of Investigation

Received by reliable electronic means and sworn and attested to by telephone on this 15th day of August 2024.



JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with joemadarats588@gmail.com, (“TARGET ACCOUNT”) that is stored at premises owned, maintained, controlled, or operated by Google LLC and Google Payment Corporation a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC and Google Payment Corporation (“Google”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on August 1, 2024, Google Reference Number: 66217208, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from June 15, 2023 until August 2, 2024, unless otherwise indicated:

- a. All business records and subscriber information, in any form kept, pertaining to the TARGET ACCOUNT, including:
 1. Names (including subscriber names, user names, and screen names);
 2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
 3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions, including log-in IP addresses;
 5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
 6. Length of service (including start date and creation IP) and types of service utilized;
 7. Means and source of payment (including any credit card or bank account number); and

8. Change history.
- b. All device information associated with the TARGET ACCOUNT, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- c. Records of user activity for each connection made to or from the TARGET ACCOUNT, including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs
- d. The contents of all emails associated with the TARGET ACCOUNT, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails.
- e. Any forwarding or fetching accounts relating to the TARGET ACCOUNT;
- f. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history.
- g. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history
- h. The contents of all text, audio, and video messages associated with the TARGET ACCOUNT, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.
- i. The contents of all records associated with the TARGET ACCOUNT in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, applications, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups; SMS data and device backups; the creation and change history of each record; accounts with access to or which

previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record.

- j. The contents of all media associated with the TARGET ACCOUNT in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.
- k. All maps data associated with the TARGET ACCOUNT, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history.
- l. All Location History and Web & App Activity indicating the location at which the TARGET ACCOUNT were active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history.
- m. All payment and transaction data associated with the TARGET ACCOUNT, such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time stamp, location data, and change history;
- n. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.
- o. All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, details of the associated device and Android ID for

each application, medium, or file; payment transactions; user settings; and all associated logs, including IP addresses, timestamps, and change history.

- p. All Google Voice records associated with the TARGET ACCOUNT, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history.

Google is hereby ordered to disclose the above information to the government within **14 days**

days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of Title 18, United States Code, Section 115 (Threatening Federal Officials), Title 18, United States Code, Section 871 (Threatening the President of the United States and Successors to the Presidency), Title 18, United States Code, Section 875(c) (Threatening Interstate Communications), and Title 18, United States Code, Section 879 (Threatening Former Presidents and Certain Other Persons), those violations involving CARILLO occurring after June 15, 2023, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Records and information relating to threats of violence directed at government officials;
- b. Records and information relating to Interstate communications related to threats of violence related to government officials;
- c. Records and information relating to steps planned or taken regarding threats of violence;
- d. Records and information relating to access of the GETTR platform, Facebook, and other social media platforms;
- e. Records and information relating to the acquisition of firearms, the planned acquisition of firearms, and the use or trade of any firearms;
- f. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files) pertaining to the communication related to target offenses;

- g. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider;
- h. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage;
- i. Any and all digital records, diaries, notes, and any other records that contain information pertaining to defendant's past travel, including but not limited to international travel completed within the last year;
- j. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- k. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;
- l. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).
- m. Any documents, communications, or financial records related to the acquisition or attempted acquisition of firearms, ammunition, and related equipment.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.